Detecting Lateral Movement in a Network for Combating Advanced Persistent Threats

Article · May 2020

CITATIONS
0

READS
730

3 authors, including:

Oluwasegun Adelaiye
Bingham University
14 PUBLICATIONS **58** CITATIONS
SEE PROFILE

Aminat Showole Ajibola
University of Abuja
25 PUBLICATIONS **61** CITATIONS
SEE PROFILE

International Journal of Information Processing and Communication (IJIPC) Vol. 9 No. 1&2 [May, 2020], pp. 209-220

Special Issue on Computing and Communication Technologies
Online: ISSN 2645-2960; Print ISSN: 2141-3959

Detecting Lateral Movement in a Network for Combating Advanced Persistent Threats

Adelaiye O. I.[1*], Ajibola A. [2], Yusuf M. [1]
[1] Bingham University, Karu, 961105, Karu, Nigeria;
[2] University of Abuja, Abuja, 902101, Abuja, Nigeria

oluwasegun.adelaiye@binghamuni.edu.ng, aminat.ajibola@uniabuja.edu.ng, yusufmusa@binghamuni.edu.ng

Abstract

Cyber security has in recent times been on the headlines and an area of great concern and threat to developed nations. These threats have metamorphosed into more advanced threats including a threat termed Advanced Persistent Threat. Advanced Persistent Threat (APT) is a highly coordinated attack method that exploits existing but unknown vulnerabilities. These adversaries are sophisticated, skilled and are highly determined to gain undetected access over an extended period and steal valuable data. APT poses high threat levels to organizations especially the government organizations. This study identified that 60% of the problem is the inability to detect penetration using traditional mitigation methods. The APT attack operates in phases which include: selecting a target, information gathering, gaining access, exploitation, operation, data discovery and collection, and data exfiltration listed from the first to the seventh phase. The fifth and sixth phase of the process deals with the lateral movement (spread) of malwares after internal reconnaissance is done. This study uses a statistical analysis approach on a dataset containing 939,394 payloads, and identifies patterns key in accurately identifying malicious verses normal data traffic. The attributes that showed a difference were source port and size in bytes. Results show that the ports used for scanning attacks are 90% unassigned ports and dynamic/private ports and, utilize data sizes of almost zero bytes. These patterns that form rules, detect the presence of APT attacks in a network. This approach is in line with CORBIT 5 and ISO no. ISO/IEC 27033-4:2014.

Keywords: *Reconnaissance, Zero-day, Information security, Intrusion detection, Malware*

1. Introduction

Information security has through the years been a challenge to information systems. The complete shift from manual methods of keeping data and information to electronic methods of storing data increases this security challenge. Information has gone from residing in stand-alone systems to distributed systems using network communication in an attempt to ease data and information sharing (Ghafir & Prenosil, 2014). Information sharing also became necessary for speedy dissemination of urgent messages and information. Electronic means of sharing information has been adopted by almost every field in an attempt to provide improved and easier methods of doing things (Alperovitch, 2011)Attacks to information systems have shown serious dangers to human coexistence and existence. An attack to RSA in 2011 cost the organization 66 million dollars asides the cost to the organizations reputation. Advanced persistent threat is a new form of attack to information systems, which is specific to organizations. This attack is carried out with high level of skill, motivation and sophistication with the aim of exfiltration of data (Brewer, 2014; Lacey, 2013).

Advanced Persistent Threat (APT) utilizes multiple vectors through a properly coordinated attack against a target. APT penetrates mostly through a group of employees in an organization by using social engineering schemes. These schemes are used to lure them to open or download attachments containing malicious contents.

Special Issue on Computing and Communication Technologies
Online: ISSN 2645-2960; Print ISSN: 2141-3959

APT is a term used for a new breed of insidious threats that use multiple stealth attack techniques and vectors to evade detection so as to gain and retain control over target systems unnoticed for long periods of time (Ovelgönne, Dumitraş, Prakash, Subrahmanian, & Wang, 2017; Tankard, 2011)

Even though APT like attacks using phishing techniques has existed over the last two decades, APT gained prominence in 2011 through a number of high profile security breaches in large global organizations in the financial, aerospace, defense, and government sector (Lopez, Alcaraz, Rodriguez, Roman, & Rubio, 2017; Yang, Zhang, Yang, Wen, & Tang, 2017)Contrary to popular belief, APT relies on normally used pre-existing techniques rather than innovative tools and techniques. But, they exploit vulnerabilities not yet known to the target system and gain long-term undetected access (Liu et al., 2014). Unlike other forms of attacks, APT attacks are premeditated targeted attacks and not noise attacks. APTs are hardly after random individuals or regular system users (Murakami, Kumano, & Koide, 2014).

APTs are not similar to other forms of attacks in the sense that they are more often based on what is called "zero-day exploits" where system and application vulnerabilities that are not yet known are exploited (Nicho, Oluwasegun, & Kamoun, 2018). This attack technique uses advanced step-by-step means of attack, which employ social engineering as a major tool to gain access. Another angle to view this though similar to the previous definitions refers to APT as a targeted attack on a network and its accompanying infrastructure. The main purpose of the attack is for the attacker to hijack information from government, financial, energy and power grids amongst others. These exploits are not necessarily for immediate gain but to have undetected access for a long period of time so as to laterally move and locate data of interest and, acquire all relevant and vital data from the organization under attack (Zhao, Wang, & Zhang, 2014).

APT is a serious challenge to organizations as current detection methods mostly fail. This is due to the fact that these methods depend largely on known signatures of attacks and APTs make heavy use of unknown loop holes to carry out attacks (Ghafir & Prenosil, 2014). Defensive tools, procedures and other controls commonly put in place to handle commodity security threats are often ineffective against targeted APT-style attacks (SecureWorks, 2013). In this respect we state our research questions:

1. Are there patterns exclusive to malicious traffic at the network plane?
2. Can these patterns be pertinent in mitigating APT?

In answering the research questions, the subsequent parts of this paper are structured as follows: Section two provides multiple viewpoints of APT in terms of APT perspectives. Section three provides related works in combating APT. Section four Outlines the materials and methods adopted. Section five provides the results of analysis done on the dataset. Section six provides analysis and discussion of the results and the research concludes in Section seven.

2. Background

In 2008, the National Institute of Standards and Technology (NIST) defined APT as “an adversary who possesses sophisticated levels of expertise and significant resources, which allow it to create opportunities to achieve its objectives by using multiple attack vectors” (Wang, Wang, Liu, & Huang, 2014). APT attacks, are more organized and have longer-term political or financial purposes unlike traditional attacks (Jeun, Lee, & Won, 2012). These adversaries usually target large corporations and foreign governments, with the objective of gaining access to confidential information or to compromise information systems. Malicious applications used in APTs when deployed stay embedded within the target machines and extract information at a slow and undetected pace (Ussath, Jaeger, Cheng, & Meinel, 2016) as well as conduct hostile cyber attacks against computers connected within the internal networks (Vert, Gonen, & Brown, 2014). Having employed stealth techniques, it continuously monitors, coordinate and steal data from specific targets in the long term while staying undetected (Lin, Ken Chang Dr Ying-Dar, 2014). Thus, in advanced persistent threat attack the adversary: (i) pursues its objectives repeatedly over an extended period of time, (ii) adapts to defenders’ efforts to resist it and (iii) is determined to maintain the level of interaction needed to execute its objectives (Chen, Desmet, & Huygens, 2014). In this

respect APT, one of the most vicious examples of a stealth threat, precisely targets unsuspecting users in organizations.

Based on the perspectives highlighted above the term 'advanced' means that the vendors are not able to catch up with the technical advancement of the perpetrators, where the perpetrators have been described as highly qualified computer specialists/scientists (rather than the traditional script kiddies) working tirelessly in some part of the world. It also implies a greatly improved method of exploiting an organization's information system for malicious intent having a very good grasp of computer intrusion techniques. The term 'persistent' shows the multi-faced and rather unrelenting continuous attempt to gain access into the organizations network using a mix of social engineering and technical skills to bypass the existing defenses. 'Persistent' also refers to deterministically gaining an extensive period of access to the target system obfuscating detection and also monitoring information within the target organization. 'Threat' refers to the magnitude of exploitable vulnerabilities facing organizations and individuals alike from APT, which is greater than the traditional cyber-attacks known to organizations. Also implies that the malicious user has a lot of resources and skill to perform the attack on the target system (Binde, McRee, & O'Connor, 2011; Hudson, 2014; Li, Huang, Wang, Fan, & Li, 2016).

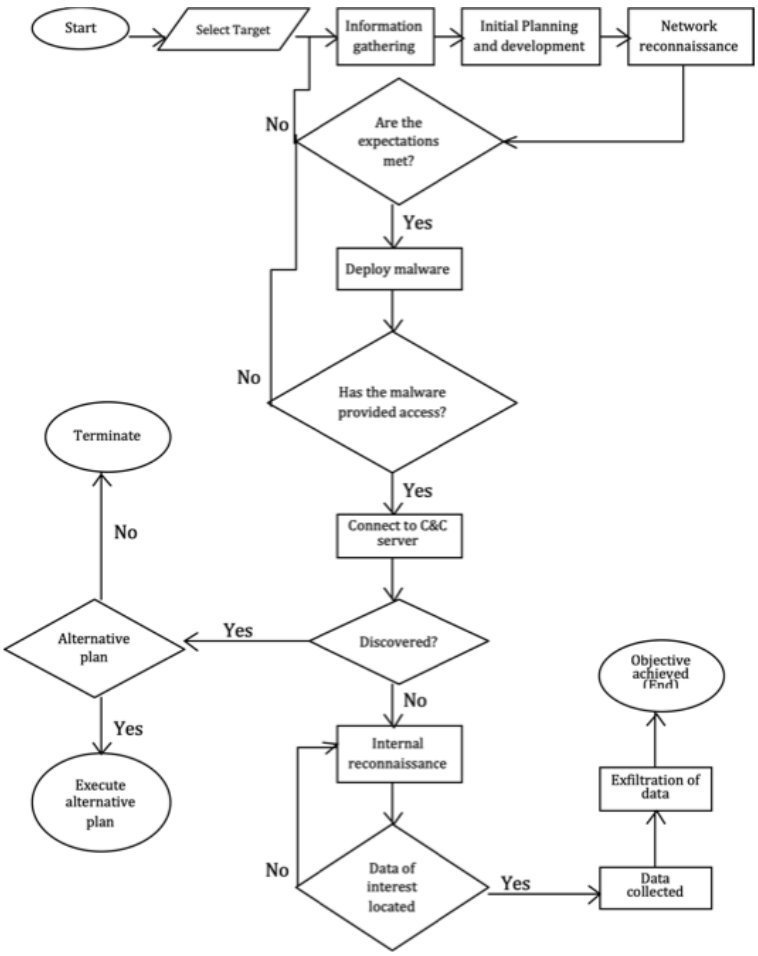


Figure 1 – APT attack process (Chen et al., 2014; Mehresh & Upadhyaya, 2016; Adelaiye, Showole, Faki 2018)

Special Issue on Computing and Communication Technologies
Online: ISSN 2645-2960; Print ISSN: 2141-3959

Comparing NIST's definition of APT, with that of other definitions by cited authors show a very similar view. Although NIST's definition shows an in-depth view of the attacks highlighting, other points like the use of multiple vectors to exploit the target, and also pointing out that the exploit might be for future use. A simple definition of APT is, a multi-layered deterministic attempt by a group of malicious and talented computer experts to exploit organizations of interest by stealing data of economic, political and financial importance. The seriousness of this exploit can be overwhelming. APT is a rapidly evolving and spreading trend multiplying and changing its form very quickly, a great challenge to organizations today (Zhao et al., 2014). Hence, many experts with respect to the extent of the attack that could earn it the APT attack title view APT differently.

In an APT attack, the victim is usually lured to either download a harmless file attachment, to click a link to a malware or an exploit-laden site through an email or to physically install a software with malicious content. When the user downloads the file, which can exploit an existing vulnerability, it installs a malware in a compromised computer, which then opens a backdoor and provides the hacker access. The attack process as shown in Figure 1 can consist of seven phases namely: target identification, information gathering, gain access, exploit, lateral movement, data discovery and collection, and exfiltration (Brewer, 2014; Chen et al., 2014; Haq, Zhai, & Pidathala, 2017).

As these attacks are not random or noise attacks, the targets are carefully selected which mostly includes government, organizations, companies etc. (Jeun et al., 2012). On selecting a target information about the target needs to be collected in detail, which will include details of the possible methods of gaining access. The information acquired at this point is very vital to the success of the attack. This phase utilizes one of three methods these include: Internal reconnaissance, external reconnaissance and methods for gaining access (Brewer, 2014).

After information has been gathered about the target organization and the best method for intrusion identified, the attacker is now set to penetrate the organization. This penetration mostly utilizes social engineering methods as well as zero-day malwares to gain access. These methods are usually successful due to the fact that social engineering uses the weakness of humans and plays on their intelligence, employing psychological skills to deceive an employer into opening or receiving messages from unidentified persons. Zero-day malwares are malicious applications that have never been seen which means there is no means of identification (Chen et al., 2014; Ghafir & Prenosil, 2014). The attacker also wants an access point to be able to issue commands from a remote location and escalate his privileges. This connection is done through what is referred to as a backdoor. This is a connection that exploits outbound filters because it is believed that all network traffic originating from within are trusted (Ask et al., 2013). Communication within a network is seen as safe and so there are little or no defenses between communications within a network. The attacker utilizes internal reconnaissance and scanning to locate the data and information sort after. The malware at this point is also spread within the network in efforts to infiltrate and locate valuable data and to spread to other vulnerable machines (Chen et al., 2014). The attack is usually well planned and the attacker has a range of assets to steal. This data of interest is collected to a single location in preparation for the exfiltration of data (Ghafir & Prenosil, 2014). At this point the data and information gathered is completely taken out to a location of choice by the attacker. At this point detection usually takes place after the data has already been stolen. The attacker is now in possession of confidential data capable of bringing dangerous risks to the organization attacked. The data/information collected usually includes authentication and authorization credentials and rights as an insider with high privileges (Chen et al., 2014).

2.1 Position of the Research

Based on the attack tree model, APT attacks can be viewed from four planes namely the physical plane, network plane, the application plane, and the user plane as indicated in Figure 2 (Giura & Wang, 2012).

Special Issue on Computing and Communication Technologies
Online: ISSN 2645-2960; Print ISSN: 2141-3959

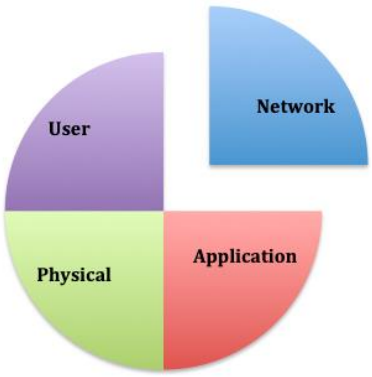


Figure 2 –Planes involved in APT attack

This research focuses mainly on the mitigation strategies at the 'network plane' targeting the 'operation' and 'data discovery" stages of an APT attack where networks play a major role. The ineffectiveness of traditional mitigation techniques in preventing against APT has cost large organizations and government agencies the loss of valuable data. Most of the methods that have been created have not been effective in detecting and/or preventing APT activities in the user, application, network or physical planes. Most researchers have attributed the successes in these attacks to human vulnerability. The ability of these malwares to bypass security mechanisms show that vulnerabilities still exists even in the midst of existing technical mitigation techniques and results in threats.

Recent studies have shown the difficulty in detecting Advanced Persistent Threats, the seriousness of APT is visible from the high profile attacks and exfiltration of data from sensitive organizations like RSA security, NASA, FBI, Sony, Citigroup, Fox broadcasting etc. (Nicho & Khan, 2014). APT operates in phase and in user, application, network and physical planes at different periods during the attack.

Our assumption is that mitigation methods can be implemented differently based on the phase and plane. This study aims at using statistical analysis to find a behavioral pattern for detecting data discovery moves and lateral movement in the network plane and the 5th and 6th phase of the attack process from within the target organization.

3. Related Work

Various authors have looked into the best techniques of detecting malicious traffic. Reves (2016) in his attempt to detect aberrant traffic, created a traffic analysis by assigning primary and secondary criteria using weights in percentage. The primary criteria dealt with source machine number of destinations and the distance from the mean number of destinations while, the secondary criteria weighed presence of bogus IP addresses, unresolved destination IP and exceeded adjacent destination addresses. Frecon et al. (2016) proposed the use of non-linear regression on packets and byte count using time series. The study showed that there exists a significant difference in byte as well as packet using the Hurst exponent. Fakuda et al. (2017) proposed the use of information about queries to classify traffic activity. The information used was based on the originator data. Fukada et al. (2017) work recorded 70-80% success in detecting malicious activity.

In looking into other malicious traffic using other traffic related activities, Houston III & Cambell (2015) proposed analysing response traffic to detect malicious activity, by mirroring traffic and sending the mirrored version for analysis by a sensor analyser in an attempt to determine if the traffic source is malicious. Curcio et al. (2017) proposed filtering portions of network based on a predefined policy that is based on the state of the network by monitoring devices on the network. Curcio et al. (2017) approach required the collection of network portions in chunks and performing analysis on these portions in an attempt to detect malicious payloads.

This study has further provided a simplified method for identifying internal reconnaissance using statistical analysis and has provided a pattern for establishing policies to detect malicious traffic.

Special Issue on Computing and Communication Technologies
Online: ISSN 2645-2960; Print ISSN: 2141-3959

4. Research Methodology

Complex systems in the physical sciences are studied by developing models of their underlying physics on a computer, and by using computationally intensive methods to learn about the behavior of those systems (Winsberg & Mirza, 2017). This research aims at reducing the chances of a successful attack through classification and pattern recognition in network data traffic.

For the purpose of this research a data set was obtained from Coburg University Germany a work done on monitoring network traffic of a business organization for 1 week using open stack. This dataset called Coburg Intrusion Detection Dataset (CIDD) consists of over 1 million records with multiple attack vectors in a CIDDS-001-internal-week1.csv file the dataset consists of 11 fields as indicated in Table 1 (Ring, Wunderlich, Grüdl, Landes, & Hotho, 2017).

Table 1. CIDDS Dataset Attributes and Description

Fields	Description
Protocol	Transport Protocol Used
Source IP Address	Source Port
Source Port No.	Source IP address
Destination IP Address	Destination IP address
Destination Port No.	Destination Port
Packets	Number of packets transmitted
Bytes	Number of Bytes transmitted
Class	Classification (Normal, Attacker and Victim
Attack Type	Attack vector used
Attack ID	Unique identification for each attack vector type
Attack Description	Details about the attack parameters

The data is analyzed to find patterns within the payload dataset for a difference using statistical analysis. The assumption is that there is a pattern in one or more fields that can prevent scanning and spreading within an organization. This approach to pattern recognition has been widely used, Reves (2016) and Kuznetsov et al. (2015) are a few amongst others, though with different variables but similar statistical techniques in detecting malicious intrusion.

Static rule-based approach to anomaly detection is used when there exist finite patterns for usual or unusual behavioral patterns. The assumption if true meets the criteria for the adoption of this approach. This approach is explained in Algorithm 1.

ALGORITHM 1
Input $V = (a_i, b_i)$ *[Indices affected by the rule applied]*
Output: anomalous traffic,
$P = \{p_1, p_2, \dots, p_n\}$ *[captured data traffic, T all data traffic within network]*
Begin
Initialize $= \{\ \} \in T\ ,\ S = \{S_1, S_2\}$ *where* S_1 *and* S_2 *are the rules threshold*
For each p_i *where* $\{a, b\} \subseteq P$
    $V \leftarrow \{a_i, b_i\}$
For each V (<, > or =) S_1*, V (<, > or =)* S_2 *and V (<, > or =)* S_3 *[*S_1*,* S_2 *and* S_3 *are predefined rules]*
If $D \leftarrow a_i = b_i$
    Return D
End

Algorithm 1 provides the process of detecting attacks using static rule based anomaly detection. The algorithm logically explains a step-by-step approach using identified patterns. The input data V, obtained from the

Special Issue on Computing and Communication Technologies
Online: ISSN 2645-2960; Print ISSN: 2141-3959

data in transit consists of the input data (a_i, b_i) required in detecting attacks. D is the detected anomalous traffic. $P = \{p_1, p_2, \dots, p_n\}$ is a subset of the entire traffic within the network. The rules S1, S2 … Sn provide thresholds to filter the traffic. The conditions is used to select the abnormal traffic and stores the suspected anomalies in D $\leftarrow a_i = b_i$. D is returned as abnormal traffic.

The condition for the implementation of the static rule based anomaly detection algorithm as shown above is through statistical analysis test for association. The test hypothesis used in obtaining the patterns is presented in 3.1.

3.1 Research Hypothesis

H_0: There is no difference between the behavioral pattern of normal and malicious traffic with respect to source port, destination port, packets and bytes.

H_1: There is a difference between the behavioral pattern of normal and malicious traffic with respect to source port, destination port, packets and bytes.

5. Results

The dataset is analyzed using SPSS v21 and Minitab 17. The dataset is categorized into three parts based on the nature of the payload. Thus, a recommended test to run is one-way analysis of variance (ANOVA).

$$F = \frac{\sum n_j(\bar{X}_j - \bar{X}) / (k-1)}{\sum\sum(X - \bar{X}_j)^2 / (N-k)} \quad \dots\dots\dots\dots\dots\dots\dots\dots (1)$$

F = the test statistic.
n_j = the sample size of the j^{th} group
$\bar{X}_j$ = Mean of j^{th} group
$\bar{X}$ = Mean
N = number of observations

Hypothesis:
$H_0: \mu_1 = \mu_2 = \cdots = \mu_n$
H_1: at least 2 μ_i are different

The data to be analyzed whose factors are similar in almost every network traffic are source and destination port, number of packet and the size in bytes.

A. Descriptive statistic of the dataset

A breakdown of the CIDD dataset is shown in **Error! Reference source not found.** using a frequency table to show the distribution of the data.

Table 2 – CIDDS Dataset Distribution

FIELD	FREQUENCY	PERCENTAGE
Normal	924862	98%
Attack	8710	1%
Victim	5822	1%
TOTAL	939394	100%

The total number of data to be analyzed is 939394 as indicated in Table 2 from the dataset due to the inability to retrieve the full data in the file, which was due to size. Table 2 shows the traffic types and the frequency, categorizing them into normal, attack and victim traffic. The attack and victim are both malicious traffic and is categorized based on the direction of the traffic.

Special Issue on Computing and Communication Technologies
Online: ISSN 2645-2960; Print ISSN: 2141-3959

B. One Way Analysis of Variance (ANOVA)

Figure 3 show that there exists a pattern in the port utilized by normal traffic, malicious traffic (attacker) and malicious traffic (victim) when an analysis of variance test is done. The ports used by attackers are mostly higher than the normal traffic and the ports exploited on the destination machines are usually much lower ports.

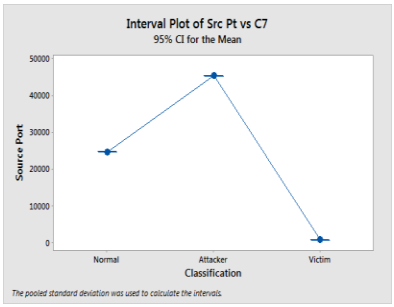


Figure 1. Source port vs classification

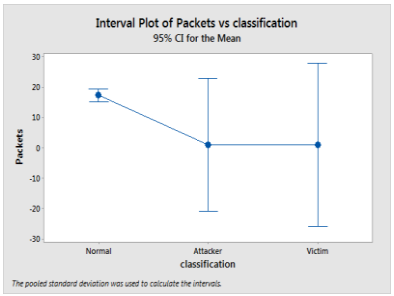


Figure 2. No. of packets vs classifications

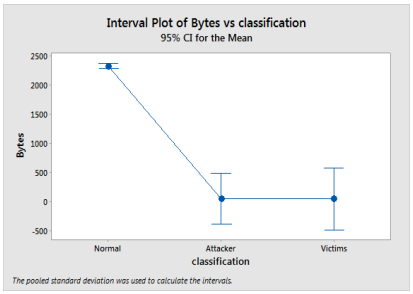


Figure 3. Size in bytes vs classification

When the interval plot is done for destination the reverse is the case. The attacker and the Victim switch position, as the payloads are replies to the attacks earlier deployed.

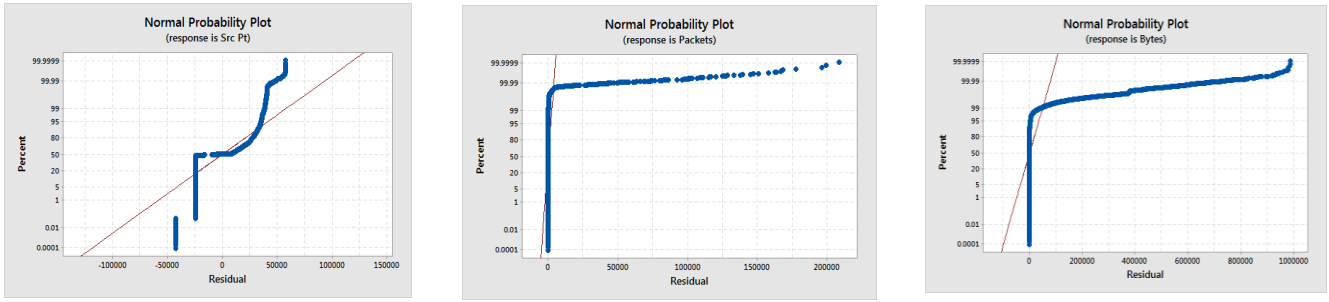
Figure 4 shows lower means for malicious traffic although the P-value of 0.176 shows that the there isn't enough reason to show a difference in the number of packets associated with either normal traffic or malicious traffic. This is evident in Figure 3 as the confidence intervals at 95% overlap each other.

With p-value of 0.00 there is strong evidence to show a difference between the normal and malicious traffic. This is evident in Figure 5. The diagram shows a wide range between the malicious traffic and normal traffic.

C. Validation of ANOVA

The test results shown above are still not admissible, as validation using a normal probability test must be done. In validating the tests done in section B. the residuals are tested for normality. Figure 6 shows the normal probability test of the three ANOVA tests done.

All the three tests do not show reasonable closeness of the points to the line hence, there is not enough evidence to show that the residuals are normal. ANOVA test is therefore invalid and nonparametric test must be used.



(a) (b) (c)

Figure 6 – Normal probability plot of residuals (a) Source port (b) Packet and (c) Bytes

Special Issue on Computing and Communication Technologies
Online: ISSN 2645-2960; Print ISSN: 2141-3959

D. Kruskal Wallis

Kruskal Wallis is a nonparametric test used to test for comparing k independent samples using population medians.

$$H = (N-1)\frac{\sum_{i=1}^{g} n_i(\bar{r}_i - \bar{r})^2}{\sum_{i=1}^{g}\sum_{j=1}^{ni}(r_{ij}-\bar{r})^2} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

H = the test statistic
N = number of observations
n_i = number of observations in i^{th} group
r_{ij} = number of observations j in i^{th} group
$\bar{r}_i$ = mean rank of observations in i^{th} group
$\bar{r} = \frac{1}{2}(N+1)$

Hypothesis:
$H_0: \eta_1 = \eta_2 = \cdots = \eta_n$
H_1: at least 2 η_i are different

The tests done in section B is repeated using Kruskal Willis, as the test results are not admissible (see section C.). The results are represented in Table 3.

Table 3 – Non parametric test results

Field	Median (Average rank Z)			Test statistic H	P-value
	Normal	Malicious(attacker)	Malicious (victim)		
Source Port	8082 (-27.27)	51357 (50.56)	2701 (-18.87)	2941.21	0.000
Packets	1.0 (98.14)	1.0 (-79.17)	1.0 (-63.76)	11357.29	0.000
Bytes	120 (173.47)	58 (-124.25)	54 (-121.05)	31357.13	0.000

1. **Source port:** p-value < 0.05. Reject H_0. There is evidence that at least 2 of the medians are different. Furthermore, the average rank (Z) for normal and victim is significantly lower than the overall mean rank (Z=-27.27<-1.96 & Z=-18.87<-1.96), and the average rank for attacker is significantly higher (Z=50.56>1.96) than the overall mean rank. We can certainly infer that the median port number for normal and victim traffic is significantly lower than the median port number for attack traffic.
2. **Packets:** p-value < 0.05. Reject H_0. There is evidence that at least 2 of the medians are different. Furthermore, the average rank (Z) for normal is significantly higher than the overall mean rank (Z=-98.14>1.96), and the average rank for malicious traffic both for victim and attacker is significantly lower (Z=-63.76<-1.96 & Z=-79.17<-1.96) than the overall mean rank. We can certainly infer that the median number of packets for normal traffic is significantly higher than the median number of packets for malicious traffic.
3. **Bytes:** p-value < 0.05. Reject H_0. There is evidence that at least 2 of the medians are different. Furthermore, the average rank (Z) for normal is significantly higher than the overall mean rank (Z=173.47>1.96), and the average rank for malicious traffic is significantly lower (Z=-124.25<-1.96 & Z=-121.05<-1.96) than the overall mean rank. We can certainly infer that the median size in bytes used in normal is significantly higher than the median bytes used for malicious traffic.

The results of the statistical analysis present rules that effectively detect the presence of malicious traffic in a network. These rules are presented below

1. Rule 1 (S_1): Flag traffic with source port within the unassigned and dynamic/private ports range.

Special Issue on Computing and Communication Technologies
Online: ISSN 2645-2960; Print ISSN: 2141-3959

2. Rule 2 (S_2): Flag traffic if size in bytes is between 0 and 58.

Having highlighted the results from the tests and obtained acceptable results meeting the criteria for the use of static rule detection, the next section discusses the implications of the results in detecting malicious traffic within a network.

6. Discussion

Advanced Persistent Threat is a skilful and highly orchestrated attack type, which follows a number of steps in completing its task. The data to be collected from the target organization mostly, do not reside in the first exploited node within that organization. The attack process is in steps as highlighted in section 3. The fifth and sixth step of the attack based on the summarized taxonomy of APT deals with spreading, lateral movement and data discovery in an attempt to locate the data sought after. This internal reconnaissance traffic has been identified as a threat to be mitigated (Curcio et al., 2017; Huston III & Campbell, 2015; Reves, 2016). The dataset used CIDDS_001.csv containing over a million instances of payloads was used although due to application and system resources we were only able to access 939,394 of these data instances. The data presented after analysis, using ANOVA showed signs of a difference in the traffic data between normal and malicious payloads as seen in Figure 2, Figure 3, Figure 4. Although in completely accepting the test results a validation of the residuals must be done which was the reason for the shift to non-parametric testing. The results of the non-parametric test showed similar results and also revealed that the ports used are unassigned or dynamic/private ports in scanning for points of intrusion. These scans are usually possible because the thought is that internal networks are safe and the fact the organizations want maximum performance and so organizations tend to allow unfiltered traffic within the network. The test on the bytes used during scanning are usually low as compared to normal traffic. This is most likely because the aim of the payload is just to identify ports. The two positive results, which show high levels of correlation in determining a pattern, are the size in bytes and the source port number. With the knowledge of these two patterns it will be easier to significantly reduce the malware spreading and the vulnerability. With these patterns based on these two fields will not be too much load on the network when implemented. These key variable determinants can easily be implemented on an intrusion detection system and also aid in the research into using machine learning based approach to detecting the presence of an APT attack. Most researchers have overlooked the potentials of mitigating APT through packet capture (PCAP) files, which provides the most basic information about network communication.

7. Conclusions

Lateral movement within a network with the aim of locating data of interest is a common trend with APT. Our solution presents a method, which uses patterns identified through statistical analysis in detecting and combating APT. From the results of the statistical analysis on the traffic data, it is evident that lateral movement of malicious applications and data can be tackled. This approach also combats the data discovery phase using source port and byte patterns. The research found that malicious traffic utilizes unassigned/dynamic ports and payload sizes are small in bytes. This is an easy method of detecting malicious traffic within an organizations network as it relies of packet header details, which are easily extractible from any network. This approach is inline with providing effective internal audit, risk management and cooperate governance as highlighted in COBIT5, an IT management and governance framework by ISACA. This approach also uses firewall techniques in securing networks as highlighted in the ISO/IEC 27033-4:2014. This standard has to do with securing communications within networks using secure gateways. Applying this solution to an organization will assist in mitigating the threat and reducing the risks bordering around APT attacks.

Special Issue on Computing and Communication Technologies
Online: ISSN 2645-2960; Print ISSN: 2141-3959

References

Alperovitch, D. (2011). Revealed: Operation shady RAT McAfee.

Ask, M., Bondarenko, P., Rekdal, J. E., Nordbø, A., Bloemerus, P., & Piatkivskyi, D. (2013). Advanced persistent threat (APT) beyond the hype. *Project Report in IMT4582 Network Security at Gjøvik University College, Springer,*

Binde, B., McRee, R., & O'Connor, T. J. (2011). Assessing outbound traffic to uncover advanced persistent threat. *SANS Institute.Whitepaper,*

Brewer, R. (2014). Advanced persistent threats: Minimising the damage. *Network Security, 2014*(4), 5-9.

Chen, P., Desmet, L., & Huygens, C. (2014). A study on advanced persistent threats. Paper presented at the *IFIP International Conference on Communications and Multimedia Security,* 63-72.

Curcio, J. A., Chiu, J., LaVigne, B. E., Lu, W., Wakumoto, S., Sanchez, M., & Laswell, M. (2017). *Monitoring Network Traffic,*

Frecon, J., Fontugne, R., Didier, G., Pustelnik, N., Fukuda, K., & Abry, P. (2016). Non-linear regression for bivariate self-similarity identification—Application to anomaly detection in internet traffic based on a joint scaling analysis of packet and byte counts. Paper presented at the *Acoustics, Speech and Signal Processing (ICASSP), 2016 IEEE International Conference On,* 4184-4188.

Fukuda, K., Heidemann, J., & Qadeer, A. (2017). Detecting malicious activity with DNS backscatter over time. *IEEE/ACM Transactions on Networking, 25*(5), 3203-3218.

Ghafir, I., & Prenosil, V. (2014). Advanced persistent threat attack detection: An overview. *International Journal of Advances in Computer Networks and its Security (IJCNS),* (I)

Giura, P., & Wang, W. (2012). Using large scale distributed computing to unveil advanced persistent threats. *Science J, 1*(3), 93-105.

Haq, T., Zhai, J., & Pidathala, V. K. (2017). *Advanced Persistent Threat (APT) Detection Center,*

Hudson, B. (2014). Advanced persistent threats: Detection, protection and prevention. *Sophos Ltd., US February,*

Huston III, L. B., & Campbell, A. (2015). *Analyzing Response Traffic to Detect a Malicious Source,*

Jeun, I., Lee, Y., & Won, D. (2012). A practical study on advanced persistent threats. *Computer Applications for Security, Control and System Engineering, 339,* 144-152.

Kuznetsov, A., Smirnov, A., Danilenko, D., & Berezovsky, A. (2015). The statistical analysis of a network traffic for the intrusion detection and prevention systems. *Telecommunications and Radio Engineering, 74*(1)

Lacey, D. (2013). *Advanced persistent threats: How to manage the risk to your business* ISACA.

Li, M., Huang, W., Wang, Y., Fan, W., & Li, J. (2016). The study of APT attack stage model. Paper presented at the *Computer and Information Science (ICIS), 2016 IEEE/ACIS 15th International Conference On,* 1-5.

Lin, Ken Chang Dr Ying-Dar. (2014). Advanced persistent threat: Malicious code hidden in PDF documents.

Liu, X., Luo, Z., Zhu, S., Kong, C., Chen, W., Nakatani, Y., . . . Shao, P. (2014). Research on prevention solution of advanced persistent threat. Paper presented at the *2014 2nd International Conference on Software Engineering, Knowledge Engineering and Information Engineering (SEKEIE 2014)). Atlantis Press,*

Lopez, J., Alcaraz, C., Rodriguez, J., Roman, R., & Rubio, J. E. (2017). Protecting industry 4.0 against advanced persistent threats. *Euro CIIP Newslett, 11*

Murakami, T., Kumano, S., & Koide, H. (2014). An implementation of tracing attacks on advanced persistent threats by using actors model. Paper presented at the *Soft Computing and Intelligent Systems (SCIS), 2014 Joint 7th International Conference on and Advanced Intelligent Systems (ISIS), 15th International Symposium On,* 1316-1320.

Nicho, M., & Khan, S. (2014). Identifying vulnerabilities of advanced persistent threats: An organizational perspective. *International Journal of Information Security and Privacy (IJISP), 8*(1), 1-18.

Nicho, M., Oluwasegun, A., & Kamoun, F. (2018). Identifying vulnerabilities in APT attacks: A simulated approach. Paper presented at the *New Technologies, Mobility and Security (NTMS), 2018 9th IFIP International Conference On,* 1-4.

Special Issue on Computing and Communication Technologies
Online: ISSN 2645-2960; Print ISSN: 2141-3959

Ovelgönne, M., Dumitraş, T., Prakash, B. A., Subrahmanian, V., & Wang, B. (2017). Understanding the relationship between human behavior and susceptibility to cyber attacks: A data-driven approach. *ACM Transactions on Intelligent Systems and Technology (TIST), 8*(4), 51.

Reves, J. P. (2016). *Traffic Anomaly Analysis for the Detection of Aberrant Network Code,*

Ring, M., Wunderlich, S., Grüdl, D., Landes, D., & Hotho, A. (2017). Flow-based benchmark data sets for intrusion detection. Paper presented at the *Proceedings of the in Proceedings of the 16th European Conference on Cyber Warfare and Security (ECCWS). 1em Plus 0.5 Em Minus,* 361-369.

SecureWorks, D. (2013). Lifecycle of the advanced persistent threat. *Cit,* , 05-11.

Tankard, C. (2011). Advanced persistent threats and how to monitor and deter them. *Network Security, 2011*(8), 16-19.

Ussath, M., Jaeger, D., Cheng, F., & Meinel, C. (2016). Advanced persistent threats: Behind the scenes. Paper presented at the *Information Science and Systems (CISS), 2016 Annual Conference On,* 181-186.

Vert, G., Gonen, B., & Brown, J. (2014). A theoretical model for detection of advanced persistent threat in networks and systems using a finite angular state velocity machine (FAST-VM). *International Journal of Computer Science and Application,*

Wang, Y., Wang, Y., Liu, J., & Huang, Z. (2014). A network gene-based framework for detecting advanced persistent threats. Paper presented at the *P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2014 Ninth International Conference On,* 97-102.

Winsberg, E., & Mirza, A. (2017). Considerations from the philosophy of simulation. *The Routledge Handbook of Scientific Realism,* , 250.

Yang, X., Zhang, T., Yang, L., Wen, L., & Tang, Y. Y. (2017). Maximizing the effectiveness of an advanced persistent threat. *arXiv Preprint arXiv:1707.02437,*

Zhao, W., Wang, P., & Zhang, F. (2014). Extended petri net-based advanced persistent threat analysis model. *Computer engineering and networking* (pp. 1297-1305) Springer